Idempotents and the BCH Bound

Daniel Augot and Nicolas Sendrier

***Abstract*— Using a characterization of the idempotents of a narrow-sense primitive binary BCH code, we are able to give classes of such codes whose minimum distance does not exceed the BCH bound. Our results are compiled in a table.**

***Index Terms*— BCH codes, minimum distance, locator polynomial, idempotents, splitting field.**

I. Introduction

We are concerned with the problem of finding the true minimum distance of binary BCH codes. This is a difficult question, and we formulate it in the following way: For a given δ, for which lengths does the BCH code of designed-distance δ and length n have true minimum distance δ? We give a partial answer by describing those BCH codes having an idempotent as a minimum-weight codeword.

We denote by $B(n, \delta)$ the narrow-sense primitive BCH code of length $n = 2^m - 1$ and designed-distance δ. In Section II, we recall the facts we need about BCH codes and locator polynomials of codewords. In Section III, we characterize idempotent codewords of $B(n, \delta)$: a word of $GF(2)^n$ of weight δ or $\delta + 1$ is an idempotent of $B(n, \delta)$ if and only if its locator polynomial can be written in the form $1 + (zp(z))^2 + z^\delta$, with $p(z) \in GF(2)[z]$ of degree at most $(\delta - 1)/2$. Thus, if such a polynomial splits in $GF(2^m)$, it is the locator polynomial of an idempotent codeword of $B(n, \delta)$ of weight δ or $\delta + 1$. This implies that $B(n, \delta)$ has minimum weight δ. In Section IV, an algorithm, along with its proof, is presented for computing the extension degree of the splitting field of a polynomial over $GF(2)$. A table of primitive narrow-sense BCH codes whose designed distance is achieved by an idempotent is produced for $\delta \leq 49$.

II. Binary BCH Codes and Locator Polynomials

A. Primitive Binary BCH Codes

We denote by $GF(q)$ the Galois field of order q, where $q = 2^m$, and denote by α a primitive nth root of unity in $GF(q)$. Any cyclic code C of length n can be defined by its *generator polynomial*, whose roots are called the zeros of the code C. Thus, we say that the defining set of C is the set

$$I(C) = \{i \in [0, n-1] | \alpha^i \text{is a zero of } C\}. \tag{1}$$

We denote by $cl(s)$ the cyclotomic class of s modulo n over $GF(2)$:

$$cl(s) = \{s, 2s, 2^2 s, \cdots, 2^{m-1} s \bmod n\}. \tag{2}$$

If α^i is a zero of C, then α^{2i} is also a zero of C, so $I(C)$ is a union of cyclotomic classes.

We are now able to give a definition of a primitive narrow-sense BCH code.

Manuscript received January 25, 1993; revised May 11, 1993.

D. Augot is with the Université Paris 6, LITP, 2 pl. Jussieu, 75251 Paris Cedex 05, France.

N. Sendrier is with the INRIA, Domaine de Voluceau, Rocquencourt, BP 105, 78153 Le Chesnay Cedex, France.

IEEE Log Number 9215186.

TABLE I
Some $B(2^m - 1, \delta)$ Codes with True Minimum Distance δ

δ	m
3	2, 3
5	4, 5, 6
7	3, 4, 7, 10
9	6, 8, 9, 10, 14, 15, 21
11	5, 6, 8, 11, 21, 28
13	8, 9, 10, 12, 13, 14, 21, 22, 33, 35
15	4, 5, 6, 7, 9, 26, 33, 39
17	8, 9, 10, 12, 14, 15, 17, 21, 35, 39, 44, 52, 55, 65, 66, 77
19	8, 9, 10, 12, 15, 19, 21, 28, 34, 35, 39, 51, 52, 65, 66, 77, 91
21	6, 7, 8, 9, 10, 11, 15, 38, 51, 57, 68, 85
23	6, 8, 10, 11, 14, 15, 21, 23, 35, 51, 52, 57, 65, 68, 76, 85, 95, 117, 119
25	8, 10, 12, 13, 15, 18, 21, 22, 25, 28, 33, 46, 57, 68, 69, 76, 77, 95, 102, 119, 133, 153
27	6, 7, 8, 9, 10, 13, 15, 33, 44, 55, 68, 69, 76, 85, 92, 115, 187
29	10, 12, 14, 15, 16, 18, 21, 25, 26, 27, 29, 35, 39, 44, 66, 68, 69, 76, 77, 92, 95, 99, 102, 114, 115, 153, 161, 171, 187, 209, 221, 715
31	5, 6, 8, 9, 14, 21, 31, 39, 44, 52, 58, 77, 87, 92, 119, 161, 209, 221, 247, 374, 561
33	10, 11, 12, 15, 16, 17, 18, 21, 27, 28, 39, 52, 62, 76, 87, 91, 92, 93, 95, 114, 115, 116, 133, 138, 145, 171, 175, 207, 247, 322
35	9, 10, 12, 14, 15, 16, 17, 21, 22, 25, 33, 35, 52, 65, 77, 78, 87, 91, 92, 93, 95, 114, 116, 124, 138, 143, 145, 152, 155, 203, 253, 299, 494, 741
37	8, 10, 12, 14, 15, 18, 19, 21, 27, 33, 34, 37, 44, 51, 52, 55, 65, 77, 78, 92, 93, 115, 116, 117, 119, 124, 138, 143, 155, 161, 174, 175, 203, 207, 217, 261, 299, 506
39	8, 9, 10, 12, 13, 15, 19, 21, 25, 28, 33, 35, 44, 51, 55, 68, 74, 77, 85, 111, 115, 116, 119, 124, 138, 145, 174, 186, 187, 217, 319, 322, 391, 406
41	10, 12, 14, 15, 16, 18, 21, 25, 26, 27, 35, 38, 39, 41, 44, 51, 57, 65, 66, 68, 77, 91, 99, 111, 116, 119, 124, 133, 138, 148, 155, 174, 184, 185, 186, 207, 209, 261, 279, 319, 341, 374, 377, 391, 437, 759, 1615, 2431
43	7, 8, 11, 12, 15, 18, 20, 27, 39, 43, 50, 52, 57, 65, 68, 76, 82, 85, 95, 102, 111, 115, 116, 123, 124, 138, 145, 148, 153, 174, 185, 186, 207, 221, 261, 279, 310, 377, 403, 437, 782, 1173
45	8, 9, 10, 11, 12, 14, 15, 21, 23, 25, 35, 39, 52, 57, 65, 68, 76, 85, 86, 91, 102, 119, 123, 124, 129, 133, 145, 148, 155, 164, 174, 186, 205, 217, 222, 247, 259, 403, 442, 493, 754
47	8, 9, 10, 12, 15, 21, 22, 23, 28, 33, 35, 47, 52, 55, 68, 76, 77, 78, 91, 95, 102, 114, 119, 123, 129, 133, 143, 148, 155, 164, 172, 174, 185, 186, 205, 215, 221, 222, 287, 325, 407, 425, 434, 493, 494, 518, 527, 551, 741, 806, 1131, 1209, 1885, 3553
49	10, 12, 14, 15, 16, 18, 21, 25, 27, 33, 35, 44, 46, 49, 52, 55, 65, 68, 69, 76, 78, 85, 94, 95, 102, 114, 117, 119, 129, 141, 143, 145, 148, 153, 164, 171, 172, 174, 186, 187, 203, 209, 215, 222, 232, 246, 248, 261, 279, 287, 299, 301, 333, 369, 407, 442, 481, 527, 551, 589, 663, 741, 986, 1131, 1209, 1479, 1771, 2387, 3059, 4199

Definition 1: For any integer $n = 2^m - 1$ and any integer $\delta > 1$, we consider the set

$$Z_{n,\delta} = \bigcup_{i=1}^{\delta-1} cl(i). \tag{3}$$

If $\delta \notin Z_{n,\delta}$, then we define the primitive narrow-sense BCH code of length n and designed-distance δ, denoted by $B(n, \delta)$, as the binary cyclic code of length n and defining set $Z_{n,\delta}$.

Remark 1: 1) If $\delta \in Z_{n,\delta}$, then $B(n, \delta)$ does not exist in our sense. Furthermore, the cyclic code of defining set $Z_{n,\delta}$ is equal to $B(n, \delta')$ for some $\delta' > \delta$.

2) A necessary and sufficient condition for $B(n, \delta)$ to exist is that δ be the smallest element of its cyclotomic class modulo n over $GF(2)$. In particular, δ must be odd.

3) The definition of $B(n, \delta)$ depends on the choice of a primitive element in $GF(2^m)$. A different choice would lead to another but equivalent code; thus the results given in Table I remain accurate.

We recall the well-known BCH bound.

Theorem 1: If the defining set of a cyclic code C contains a set of $\delta - 1$ consecutive integers (0 is treated consecutive to $n - 1$), then the minimum distance of C is at least δ.

We are concerned with the problem of finding the true minimum distance of $B(n, \delta)$. First, we state the following fact.

Remark 2: If $B(n, \delta)$ contains a word of even weight w, then by action of the automorphism group of the extended code (see [2, p.

236, Theorem 16]), $B(n, \delta)$ contains a word of odd weight $w-1$. Thus, the true minimum distance of $B(n, \delta)$ is odd.

B. Locator Polynomials

For this section, all details can be found in [2, ch. 8, sect. 6 and ch. 9, sect. 2]. We denote by R_n the quotient ring $GF(2)[x]/(x^n-1)$.

Definition 2: Let $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^n$ be an element of R_n of Hamming weight w. The locators of $c(x)$ are the elements $X_1 = \alpha^{j_1}, \cdots, X_w = \alpha^{j_w}$ of $GF(2^m)$ where $c_{j_1}, \cdots, c_{j_w}$ are the nonzero coefficients of $c(x)$.

The locator polynomial of $c(x)$ is the following polynomial of $GF(2^m)[z]$:

$$\sigma(z) = \prod_{i=1}^{w}(1 - zX_i).$$

The form of the locator polynomial of a word in R_n gives a necessary and sufficient condition for this word to belong to $B(n, \delta)$.

Proposition 1: Let δ be an odd integer, and let $\sigma(z) = \sigma_0 + \cdots + \sigma_w z^w$ be the locator polynomial of an element $c(x)$ of R_n of weight $w \geq \delta$.

1) *We have*

$$c(\alpha) = \cdots = c(\alpha^{\delta-1}) = 0 \Leftrightarrow \sigma_i = 0 \quad \text{for all odd } i, 1 \leq i < \delta. \quad (4)$$

2) *Furthermore, if $w = \delta$ or $w = \delta + 1$ and $c(x)$ satisfies either side of the equivalence (4), then $B(n, \delta)$ exists and has minimum distance δ.*

Proof:

1) For an integer $j \geq 0$, set $A_j = c(\alpha^j)$. The first w Newton identities for $c(x)$ are

$$\begin{cases} I_1: A_1 + \sigma_1 = 0 \\ I_2: A_2 + A_1\sigma_1 + 2\sigma_2 = 0 \\ \quad\vdots \qquad\qquad\vdots \\ I_r: A_r + \sum_{i=1}^{r-1} A_{r-i}\sigma_i + r\sigma_r = 0 \\ \quad\vdots \qquad\qquad\vdots \\ I_w: A_w + \sum_{i=1}^{w-1} A_{w-i}\sigma_i + w\sigma_w = 0. \end{cases}$$

a) Suppose we have $A_1 = \cdots = A_{\delta-1} = 0$. Since $w \geq \delta$, for all odd $r < \delta$, we have $\sigma_r = 0$ from I_r.

b) Suppose $\sigma_r = 0$ for all odd $r < \delta$. We prove by induction on r that $A_r = 0$ for $r < w$.

i) From I_1, we have $A_1 = 0$.

ii) Let $r < \delta$, and suppose $A_1 = \cdots = A_{r-1} = 0$. The identity I_r gives $A_r = 0$ for both odd and even r.

2) We suppose that $c(x)$ satisfies (4) and has weight $w = \delta$ or $w = \delta + 1$.

From Remark 1, $c(x)$ is in the code $B(n, \delta')$ for some $\delta' \geq \delta$. Let d be the minimum distance of $B(n, \delta')$. From the BCH bound and the definition of the minimum distance, we have $w \geq d \geq \delta'$, so $\delta + 1 \geq d \geq \delta'$. Since δ and δ' are both odd, this inequality implies $\delta \geq \delta'$; thus, $\delta = \delta'$. This proves the existence of $B(n, \delta)$.

If $w = \delta$, $c(x)$ is a word of weight δ. If $w = \delta + 1$ is even, by Remark 2, there is a word in $B(n, \delta)$ of weight δ. In both cases, $d = \delta$. □

III. The Characterization of Idempotents of $B(n, \delta)$

Definition 3: An idempotent $p(x)$ of R_n is a polynomial such that $p(x)^2 = p(x)$.

Proposition 2 [1, Lemma 2]: Let $\sigma(z)$ be the locator polynomial of $c(x)$ in R_n. Then $c(x)$ is an idempotent if and only if $\sigma(z)$ has all its coefficients in GF(2).

Definition 4: The splitting field of a polynomial $p(x)$ of $GF(q)[x]$ is the smallest extension of $GF(q)$ containing all the roots of $p(x)$.

Theorem 2: Let δ be an odd integer. There exists a polynomial $\sigma(z) = \sigma_0 + \cdots + \sigma_w z^w$ in $GF(2)[z]$ satisfying

$$\begin{cases} \deg\sigma \in \{\delta, \delta+1\} \\ \sigma_\delta = \sigma_0 = 1 \\ \text{for all odd } i, 1 \leq i < \delta, \sigma_i = 0 \end{cases} \quad (5)$$

that splits in $GF(2^m)$ if and only if $B(n, \delta)$, $n = 2^m - 1$ exists and contains an idempotent codeword of weight δ or $\delta + 1$.

This idempotent codeword is precisely the element of R_n whose locator polynomial is $\sigma(z)$.

Proof:

1) Suppose that $\sigma(z) \in GF(2)[z]$ splits in $GF(2^m)$.

- Since $\sigma'(z) = d/dz\sigma(z) = z^{\delta-1}$, we have $\gcd\left(\sigma'(z), \sigma(z)\right) = 1$, so $\sigma(z)$ has no multiple roots.
- $\sigma_0 = 1$, so 0 is not a root of $\sigma(z)$. Since $\sigma(z)$ splits in $GF(2^m)$, it is the locator polynomial of some idempotent element $c(x)$ of R_n, $n = 2^m - 1$.
- From Proposition 1, it follows that $B(n, \delta)$ exists and has minimum distance δ, and we have $c(x) \in B(n, \delta)$.

2) Reciprocally, if $B(n, \delta)$ exists and contains an idempotent codeword of weight δ or $\delta + 1$.

- From Proposition 2, the locator polynomial $\sigma(z)$ of this codeword is in $GF(2)[z]$ and has degree δ or $\delta + 1$.
- From Proposition 1, $\sigma_i = 0$ for all odd i, $1 \leq i < \delta$.
- Any locator polynomial of an element of R_n splits in $GF(2^m)$ and is such that $\sigma_0 = 1$.
- Finally, σ_δ=0 would imply that $\sigma(z)$ is a square; thus, σ_δ=1, and $\sigma(z)$ satisfies (5). □

Proposition 3: A polynomial $\sigma(z)$ of $GF(2)[z]$ satisfies (5) if and only if it is equal to $1 + (zp(z))^2 + z^\delta$ for some polynomial $p(z)$ in $GF(2)[z]$ of degree lower or equal to $(\delta - 1)/2$.

Proof: If $\sigma(z) \in GF(2)[z]$ and $\sigma(z) = 1 + (zp(z))^2 + z^\delta$ with $p(z) \in GF(2)[z]$ of degree at most $(\delta-1)/2$, then $\sigma(z)$ has no term of odd degree except z^δ, and we clearly have $\sigma_0 = \sigma_\delta = 1$ as well as the degree condition.

Reciprocally, if $\sigma(z)$ satisfies (5), then its only odd degree term is z^δ, so $\sigma(z) - z^\delta$ only has even degree term, and thus can be written $1 + (zp(z))^2$ for some polynomial of $GF(2)[z]$. The degree condition is easy to check. □

Thus, Theorem 2 states that for any odd δ, if we are able to find a polynomial $p(z)$ in $GF(2)[z]$ of degree at most $(\delta-1)/2$ that splits in $GF(2^m)$, then the code $B(2^m-1, \delta)$ exists and contains a codeword of weight δ or $\delta+1$. Since the true minimum distance of a primitive narrow-sense BCH code is odd, this proves that $B(2^m - 1, \delta)$ has minimum distance δ.

Rather than look for a polynomial $1 + (zp(z))^2 + z^\delta$ that splits in a given field, we will instead look efficiently for the splitting field of any such polynomial. In order to do this, we must be able to find the splitting field of a given polynomial.

IV. Binary Codes with Minimum-Weight Idempotents

A. Finding the Splitting Field of a Polynomial of $GF(2)[z]$

We present here an algorithm that computes the splitting field of a polynomial $\sigma(z)$ of $GF(2)[z]$.

Algorithm 1

INPUT: *a polynomial* $\sigma(z)$ *in* $GF(2)[z]$

1) $s_0(z) = \sigma(z)$, $p_0(z) = z$

2) *for all* $i \geq 0$, *while* $s_i(z) \neq 1$, $\begin{cases} p_{i+1}(z) = p_i(z)^2 \bmod s_i(z) \\ r_{i+1}(z) = \gcd(s_i(z), \\ \quad p_{i+1}(z) - z) \\ s_{i+1}(z) = \frac{s_i(z)}{r_{i+1}(z)} \end{cases}$

3) *let* $I = \{i, 1 \leq i \leq i_0 \mid r_i(z) \neq 1\}$, *where* i_0 *is the smallest index such that* $s_{i_0}(z) = 1$.

OUTPUT: $\operatorname{lcm}(I)$ *(lowest common multiple)*

The following lemmas describe the algorithm whose correct behavior is stated by Proposition 4.

Lemma 1: For all i, $1 \leq i \leq i_0$, *we have*

$$p_i(z) = z^{2^i} \bmod s_{i-1}(z). \tag{6}$$

Proof:

1) For $i = 1$, $p_1(z) = p_0(z)^2 \bmod s_0(z) = z^2 \bmod s_0(z)$.

2) For $i \geq 1$, we suppose we have $p_i(z) = z^{2^i} \bmod s_{i-1}(z) = z^{2^i} + \lambda(z)s_{i-1}(z)$; then

$$\begin{aligned} p_{i+1}(z) &= p_i(z)^2 \bmod s_i(z) \\ &= (z^{2^i} + \lambda(z)s_{i-1}(z))^2 \bmod s_i(z) \\ &= (z^{2^i} + \lambda(z)r_i(z)s_i(z))^2 \bmod s_i(z) \\ &= z^{2^{i+1}} \bmod s_i(z). \end{aligned}$$

□

Lemma 2: For all i, $1 \leq i \leq i_0$, $s_i(z)$ *is the product of all irreducible factors of* $\sigma(z)$ *of degree* $> i$.

Proof: We prove the result by induction on i.

1) For $i = 1$, we have $r_1(z) = \gcd(z^2 - z, \sigma(z))$ and $s_1(z) = \sigma(z)/r_1(z)$, so the result holds for $s_1(z)$.

2) For $i > 1$, we have $s_i(z) = s_{i-1}(z)/r_i(z)$, where $r_i(z) = \gcd(s_{i-1}(z), z^{2^i} - z)$. All irreducible polynomials of degree i are factors of $z^{2^i} - z$; thus, the irreducible factors of $s_i(z)$ are exactly the factors of $s_{i-1}(z)$, except those of degree i. □

Lemma 3: For all i, $1 \leq i \leq i_0$, $r_i(z)$ *is the product of the irreducible factors of* $\sigma(z)$ *of degree* i.

Proof: This result is a consequence of Lemma 2 and of the relation $r_i(z) = s_{i-1}(z)/s_i(z)$. □

Proposition 4: Algorithm 1 always halts, and the integer it returns for the input $\sigma(z)$ *is the extension degree of the splitting field of* $\sigma(z)$.

Proof: The polynomial $\sigma(z)$ has no factor of degree $> \delta$; thus, from Lemma 2, $s_\delta(z) = 1$. So $i_0 \leq \delta$, and the algorithm halts.

From the construction of the $r_i(z)$, we have

$$\sigma(z) = \prod_{i=1}^{i_0} r_i(z)$$

so the smallest field containing all the roots of $\sigma(z)$ is the smallest field containing all the roots of the $r_i(z)$'s.

By Lemma 3, the smallest field containing the roots of $r_i(z) \neq 1$ is $GF(2^i)$. Thus, if $I = \{i, 1 \leq i \leq i_0 \mid r_i(z) \neq 1\}$, the splitting field of $\sigma(z)$ is the smallest field containing $GF(2^i)$ for all i in I, that is, $GF(2^m)$ where $m = \operatorname{lcm} I$. □

Algorithmic Complexity: We will use the notations of Algorithm 1.

The number of loops of the algorithm is bounded by δ; we are assured that $s_\delta(z) = 1$ since $\sigma(z)$ has no factor of degree $> \delta$.

For each loop, we have to

1) compute the remainder of a polynomial of degree at most 2δ divided by a polynomial of degree at most δ,

2) compute the gcd of two polynomials of degree at most δ,

3) compute the quotient of two polynomials of degree at most δ.

This leads to a worst case complexity bounded by $O(\delta^2)$. Considering the number of loops, the number of basic operations is bounded by $O(\delta^3)$, where the basic operation is an addition or a multiplication in $GF(2)$.

B. A Table of Primitive BCH Codes Whose Minimum Distance Does Not Exceed theBCH Bound

For any given δ, using Algorithm 1, we compute the extension degree of the splitting field of the polynomials $\sigma(z) = 1 + (zp(z))^2 + z^\delta$ for all $p(z) \in GF(2)[z]$ of degree $\leq (\delta - 1)/2$. Let M_δ be the set of all the integers obtained. From Theorem 2, for all m in M_δ, the code $B(2^m - 1, \delta)$ exists and has minimum distance δ.

In Table I, we give the values of all $m \in M_\delta$ for all odd δ between 3 and 49. We thus have a list of binary primitive narrow-sense BCH codes whose minimum distance is the designed distance.

Remark 3: If m' is in M_δ, then for any multiple m of m', $B(2^m - 1, \delta)$ exists and has minimum distance δ. Thus, the values of $m \in M_\delta$ for which we already had an integer $m' < m$, $m' \mid m$ and $m' \in M_\delta$ were removed from Table I. For instance, for $\delta = 7$, all codes $B(2^m - 1, 7)$, with m a multiple of 3, 4, 7, or 10, have an idempotent of weight 7 or 8.

V. Concluding Remarks

The number of polynomials of the form $1 + (zp(z))^2 + z^\delta$ to investigate is $2^{(\delta+1)/2}$. The total complexity is thus about $O(\delta^3 2^{(\delta+1)/2})$ bit operations.

Considering this complexity, we have limited the search to $\delta \leq 49$, which appeared to be the limit for a reasonable computing effort.

It has to be pointed out that the above complexity is independent of the length of the code. For instance, the largest nontrivial code we found whose minimum distance is the designed distance is the code $B(2^{4199-1}, 49)$. It is nontrivial in the sense that the result is not derived from another code of shorter length.

We are able to give the true minimum distance of many BCH codes of relatively large length and dimension; this kind of result would have been very difficult to achieve with other techniques such as those employed for the tables [3, pp. 493–534] or [4, Table I]. For instance, by associating results from Table I with known facts, for length 511 and 1023 and $\delta \leq 49$, we have the following.

$m = 9$, $n = 511$

- For $\delta \in \{33, 49\}$, $B(511, \delta)$ does not exist.
- For $\delta \in \{3, 7, 13, 15, 17, 19, 21, 27, 31, 35, 39, 45, 47\}$, $B(511, \delta)$ has an idempotent codeword of weight δ or $\delta + 1$.
- For $\delta \in \{5, 9, 11, 23, 25\}$, $B(511, \delta)$ has a codeword of weight δ.
- For $\delta \in \{29, 37, 41, 43\}$, the true minimum distance is unknown.

$m = 10$, $n = 1023$

- The code $B(1023, \delta)$ exists for odd δ less than or equal to 49.
- For all $\delta \neq 43$, $B(1023, \delta)$ has an idempotent codeword of weight δ or $\delta + 1$.
- The true minimum distance of $B(1023, 43)$ is unknown.

It appears that looking for idempotent codewords of minimum weight is often successful for primitive narrow-sense BCH codes, at least for short length. We have not, as yet, found any satisfactory reason for this behavior.

ACKNOWLEDGMENT

The authors wish to thank Prof. E. F. Assmus for his careful and patient reading which improved the quality of the paper.

REFERENCES

[1] D. Augot, P. Charpin, and N. Sendrier, "Studying the locator polynomials of minimum weight codewords of BCH codes," *IEEE Trans. Inform. Theory*, vol. 38, pp. 960–973, May 1992.
[2] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*. Amsterdam: North-Holland, 1977.
[3] W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes*. Cambridge, MA: M.I.T. Press, 1972.
[4] J. H. van Lint and R. M. Wilson, "On the minimum distance of cyclic codes," *IEEE Trans. Inform. Theory*, vol. IT-32, pp. 23–40, Jan. 1986.

Codes Over Gaussian Integers

Klaus Huber

***Abstract*—In this contribution it is shown how block codes over Gaussian integers can be used for coding over two-dimensional signal space. We introduce a two-dimensional modular distance called Mannheim distance and propose using codes designed for this distance. Some simple constructions of such codes are given, among them icyclic codes which belong to the class of constacyclic codes. As a special case icyclic codes include perfect one Mannheim error correcting codes. For most of the codes considered efficient decoders are given and their performance on the Gaussian channel is investigated.**

***Index Terms*— Block codes, Gaussian integers, sum of two squares, Manhattan distance, Mannheim distance, QAM signal constellations.**

I. INTRODUCTION

It is well known that the beautiful algebraic theory of block codes over finite fields does have severe problems with coding for two-dimensional signal constellations such as quadrature amplitude modulation (QAM). This is mainly due to the fact that in two (or higher) dimensions the usual Hamming distance is inappropriate. For phase shift keyed (PSK) signals block codes using the Lee distance provide a good solution, whereas neither Hamming nor Lee distance are adequate for handling QAM signals.

To improve the situation in the two-dimensional case we introduce the Mannheim distance which is the Manhattan distance modulo a two-dimensional grid.

Then we propose block codes over Gaussian integers designed for the Mannheim distance which are suited for QAM signals. The main class of codes considered are icyclic codes which belong to the class of constacyclic codes ([1, p. 303]). We show the power of these codes when used with the Mannheim metric. First decoders are developed which are able to correct Mannheim errors of weight one and two. These decoders work in a similar way as the decoders for negacyclic codes for the Lee distance given by Berlekamp in ([1, pp. 207–217]). Then codes are considered which can correct more than two Mannheim errors. The gain of the codes on a Gaussian channel is also investigated.

Manuscript received May 21, 1992. This work was presented in part at CDS-92 Conference, Kaliningrad (Königsberg), Russia, September 7–11, 1992, and at the IEEE Symposium on Information Theory, San Antonio, TX, January 17–22, 1993.

The author is with Deutsche Bundespost Telekom, Research Institute FZ123a, 64276 Darmstadt, Germany.

IEEE Log Number 9215213.

II. CODES OVER GAUSSIAN INTEGERS

Gaussian integers are a subset of complex numbers which have integers as real and imaginary parts. Fermat's well-known and famous two square theorem tells us that primes of the form $p \equiv 1 \bmod 4$ can be written in essentially one way as a sum of two squares (see, e.g., [3, Theorem 251]). Hence such primes p are the product of two conjugate complex Gaussian integers:

$$p = a^2 + b^2 = \pi \cdot \pi^* \tag{1}$$

where $\pi = a + i \cdot b$ and the conjugate of π is $\pi^* = a - i \cdot b$. The properties of Gaussian integers as relevant for this paper are listed in Appendix E, for further details see, e.g., [3, pp. 182–187], a fast algorithm to compute a and b for a given p can be found in Appendix F. Let $\mathcal{G}$ be the Gaussian Integers and $\mathcal{G}_\pi$ the residue class of $\mathcal{G}$ modulo π, where the modulo function μ: $\mathcal{G} \rightarrow \mathcal{G}_\pi$ is defined according to

$$\mu(\xi) = \xi \bmod \pi = \eta = \xi - \left[\frac{\xi \cdot \pi^*}{\pi \cdot \pi^*}\right] \cdot \pi. \tag{2}$$

$[\cdot]$ denotes rounding of complex numbers which is defined in Appendix E such that the norm of η is as small as possible (i.e., the energy of the corresponding signal point is as small as possible). In Figs. 1–6 the sets $\mathcal{G}_\pi$ obtained from the primes $p = 5$, 13, 17, 29, 37, and 41 are displayed as points in the complex plane. Having coding for communication channels in mind we call these two-dimensional visualisations of $\mathcal{G}_\pi$ by the communication term *signal constellation*. Similarly, as for ordinary integers, we can employ the extended Euclidean algorithm for Gaussian integers to compute u and v which fulfill

$$1 = u \cdot \pi + v \cdot \pi^*. \tag{3}$$

Table VIII gives π, u, and v for the primes $p \equiv 1 \bmod 4$ and $p \leq 113$. The modulo function μ defines a bijective mapping from $GF(p)$ into two-dimensional signal space μ: $GF(p) \rightarrow \mathcal{G}_\pi$

$$\mu(g) = g \bmod \pi = \gamma = g - \left[\frac{g \cdot \pi^*}{p}\right] \cdot \pi. \tag{4}$$

Using (3) we immediately get the inverse mapping μ^{-1} as

$$g = \mu^{-1}(\gamma) \equiv \gamma \cdot (v\pi^*) + \gamma^* \cdot (u\pi) \bmod p, \tag{5}$$

for if g is an integer of $GF(p)$ then $g = \kappa \cdot \pi + \gamma$ and $g = g^* = \kappa^* \cdot \pi^* + \gamma^*$, hence, $\gamma \cdot (v\pi^*) + \gamma^* \cdot (u\pi) = (g - \kappa\pi) \cdot (v\pi^*) + (g - \kappa^*\pi^*) \cdot (u\pi) \equiv g \cdot (v\pi^* + u\pi) \bmod p$ which equals g by (3).

Clearly, μ defines an isomorphism, namely, $\mu(g_1 + g_2) = \mu(g_1) + \mu(g_2)$ and $\mu(g_1 \cdot g_2) = \mu(g_1) \cdot \mu(g_2)$. Although $GF(p)$ and $\mathcal{G}_\pi$ are equivalent mathematically, we will see in the following sections that the field $GF(p)$ when represented as $\mathcal{G}_\pi$ offers significant technical advantages for coding over two-dimensional signal space. We therefore use $\mathcal{G}_\pi$ to stress this fact.

We now define a block code $\mathcal{C}$ of length n over the Gaussian integers $\mathcal{G}_\pi$ as a set of codewords $\boldsymbol{c} = (c_0, c_1, \cdots, c_{n-1})$ with coefficients $c_i \in \mathcal{G}_\pi$. In the following, we will mainly consider linear codes.